

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Avaya IP Office Customer Call Reporter

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-365>

Gestion du document

Référence	CERTA-2012-AVI-365
Titre	Vulnérabilité dans Avaya IP Office Customer Call Reporter
Date de la première version	04 juillet 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité AVAYA 100164021 du 28 juin 2012
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Exécution de code arbitraire à distance.

2 Systèmes affectés

- Versions antérieures à Avaya IP Office Customer Call Reporter 7.0.5.8 pour la branche 7.0 ;
- versions antérieures à Avaya IP Office Customer Call Reporter 8.0.9.13 pour la branche 8.0.

3 Résumé

Une vulnérabilité a été corrigée dans *Avaya IP Office Customer Call Reporter*. Elle permet à un utilisateur non authentifié de pouvoir envoyer des fichiers arbitraires sur le serveur au moyen de « ImageUpload.ashx ». Ainsi un attaquant peut exécuter du code arbitraire à distance.

4 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 Documentation

- Bulletin de sécurité AVAYA 100164021 du 28 juin 2012 :
<https://downloads.avaya.com/css/P8/documents/100164021>
- Référence CVE CVE-2012-3811 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3811>

Gestion détaillée du document

04 juillet 2012 version initiale.